課題番号１４４

マルウェア対策ユーザサポートシステムの研究開発

一般のPCユーザ向けに、高度化･巧妙化するマルウェアに柔軟に対応可能な、総合的なセキュリティユーザサポートシステムを新たに構築することを目的として、nicterシステムとの連携を基本としつつ、以下に示す３つの機能を取り込んだシステムを実現するための研究開発を実施する。

①フォールスポジティブの発想の下で、マルウェアに該当する可能性があるプログラムを出来る限り幅広くかつ高精度に検出する機能
②nicterシステムが提供する「ミクロ解析システム」を有効に活用し、効果的に連携していく機能
③上記②の解析結果に基づき、必要となる駆除ツールを生成し、それを感染に該当するユーザに対して迅速に提供していく機能

＊注1：フォールスポジティブ ・・・・・ 不正でない対象を、“不正”と誤判定することを許す状態。
＊注2：nicter ・・・・・ 情報通信研究機構（NICT）では、広域のネットワークを想定し、スキャンを中心とした攻撃検知とその原因となり得るマルウェア等の解析により、インシデントを迅速かつ正確に検知し、対策を導出するための研究開発を行うために、nicterと呼ばれるインシデント分析センターの構築を進めている。

研究開発期間：平成２１年度～平成２３年度（3年間）
予算：２３７百万円程度（平成２１年度、上限）

課題ア：検査プログラムに関する研究開発

課題アー１　不正プログラム基本探索アルゴリズムに関する研究開発
課題アー２　ホワイトリスト化等を用いた高能率探索手法に関する研究開発

課題イ：マルウェア駆除ツールの自動生成･最適化･高速検証手法の研究開発

課題イー１　マルウェア駆除ツールの自動生成･最適化手法の研究開発
課題イー２　マルウェア駆除ツールの安全性の高速検証手法の研究開発

課題ウ：ユーザサポートプロトコルに関する研究開発

課題ウー１　クライアントサーバプロトコルの設計及び開発
課題ウー２　クライアントサーバエージェントの設計及び開発

課題エ：課題ア～ウを実環境で有効に機能させるための実証実験

本研究開発の全体アーキテクチャ